CLAIMS

What is claimed is:

1. A method of managing a network, said method comprising:

a) receiving a packet at a first port in said network, wherein;

b) determining if an address associated with said packet is authorized for said first port; and

c) forwarding said packet if said address is authorized.

2. The method of Claim 1, further comprising:

d) dropping said packet if said address is not authorized.

3. The method of Claim 1, wherein a) comprises receiving said packet from a device coupled to said first port, said first port being a switch port, and wherein there is a one-to-one mapping between ports of devices in said network and ports of switches in said network.

4. The method of Claim 1, wherein c) comprises forwarding said packet to a device if said address is authorized for said first port, said first port coupled to said device, and wherein said network comprises a virtually-wired switching fabric.

5. The method of Claim 1, further comprising:

d) comparing a set of learned addresses against a set of expected addresses, said learned addresses comprising addresses associated with packets received at a second port, said expected addresses derived from an expected configuration of said network.

6. The method of Claim 5 wherein said second port couples two switches in a virtually-wired switching fabric.

7. The method of Claim 6, further comprising:

e) tracing a topology of said network to find a third port where an unexpected address entered said virtually-wired switching fabric.

8. The method of Claim 7, further comprising:

f) taking corrective action at said third port, said third port coupled to a device.

9. The method of Claim 8, wherein f) comprises disabling said third port.

10. The method of Claim 1, further comprising:

d) determining changes in physical topology of said network.

11. The method of Claim 10 wherein d) comprises comparing a physical description of said network with a stored physical description of said network.

12. The method of Claim 1 wherein said address is a media access control (MAC) address.

13. A computer-readable medium having stored thereon a program, which when run on a processor, performs a method of managing a network, said method comprising:

a) comparing addresses associated with packets received at a first port in said network with expected addresses for said first port to determine unexpected addresses; and

b) locating a second port in said network that is a source of an unexpected address if said unexpected address is detected.

14. The computer-readable medium of Claim 13 wherein said network is a virtually-wired switching network and said first port couples switches in said network and said second port is coupled to a host device.

15. The computer-readable medium of Claim 13, wherein b) of said method comprises tracing a topology of said network to determine said second port, wherein said network comprises a virtually-wired switching fabric and said second port is at the edge of said fabric.

16. The computer-readable medium of Claim 15, wherein said method further comprises:

c) taking corrective action at said second port, wherein said second port is coupled to a host device.

17. The computer-readable medium of Claim 15, wherein said method further comprises:

c) disabling said second port, wherein said network is a virtually-wired switching fabric and said second port is at the edge of said fabric.

18. The computer-readable medium of Claim 13 wherein a) of said method comprises reading a bridge table to determine learned addresses at said first port.

19. The computer-readable medium of Claim 13 wherein a) of said method is repeated for each interconnect port in said network, wherein said network comprises a plurality of switches.

20. The computer-readable medium of Claim 13, wherein said method further comprises:

c) determining changes in physical topology of said network.

21. The computer-readable medium of Claim 20 wherein c) of said method comprises comparing a physical description of said network with a stored physical description of said network.

22. A method of managing a network, said method comprising:

a) configuring a switch in said network to forward a packet received at a first port if an address associated with said packet is authorized for said first port;

b) forwarding said packet if said address is authorized; and

c) comparing a set of learned addresses against a set of expected addresses, said learned addresses comprising addresses associated with packets processed at a second port, said expected addresses derived from an expected configuration of said network.

23. The method of Claim 22, further comprising:

d) tracing a topology of said network to find a third port where an unexpected address entered said network, said third port coupled to a device having a media access control (MAC address) that is said unexpected address.

24. The method of Claim 23, further comprising:

e) disabling said third port, wherein said network is a virtually-wired switching fabric and said third port is at the edge of said fabric.

25. The method of Claim 22, further comprising:

d) dropping said packet if said address is not authorized.

26. The method of Claim 22, wherein a) comprises programming a switch in said network to recognize authorized addresses for said first port.

27. The method of Claim 22, wherein b) further comprises forwarding said packet to a host device if said address is authorized for said first port, said first port coupled to said host device.

28. The method of Claim 22, further comprising:

d) determining changes in physical topology of said network.

29. The method Claim 28 wherein d) comprises comparing a physical description of said network with a stored physical description of said network.

30. The method of Claim 29 wherein said address is a media access control (MAC) address and wherein said network comprises a virtually-wired switching fabric.

31. A network comprising:

a plurality switches;

said switches interconnected and configured to control communication between a plurality of devices coupled to said network; and

a first switch of said plurality configured to detect a packet having an unauthorized media access control (MAC) address.

32. The network of Claim 31, wherein:

said first switch is further configured to forward said packet if said address is authorized.

33. The network of Claim 31, wherein:

said first switch is further configured to drop said packet if said address is not authorized.

34. The network of Claim 31, wherein there is a one-to-one mapping between ports of said switches and ports of said devices.